CLAIMS

What is claimed is:

1. A method of processing messages, comprising:

comparing a nonce value of a received message with a largest nonce value yet seen;

comparing said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen; and

rejecting said received message in response to said nonce value falling outside said acceptance window.

2. The method according to claim 1, further comprising:

designating said nonce value as a nonce value seen in response to said nonce value exceeding said largest nonce value yet seen.

3. The method according to claim 1, further comprising:

replacing said largest nonce value yet seen with said nonce value in response to said nonce value exceeding said largest nonce value yet seen.

4. The method according to claim 1, further comprising:

adjusting an acceptance window based on said nonce value in response to said nonce value exceeding said largest nonce value yet seen.

5. The method according to claim 1, further comprising designating said received message as a replay attack.

6. The method according to claim 1, further comprising:

comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

rejecting said received message in response to an outcome of said comparison of said nonce value to said window mask value being true.

7. The method according to claim 6, further comprising:

designating said received message as part of a replay attack.

8. The method according to claim 1, further comprising:

comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

accepting said received message in response to an outcome of said comparison of said nonce value to said window mask value being false.

9. The method according to claim 8, further comprising: designating said nonce value as a nonce value seen.

10. An apparatus for processing messages, said apparatus comprising:

a communication interface configured to transmit and receive a plurality of packets; and

a controller, wherein said controller is configured to:

compare a nonce value of a received message and a largest nonce value yet seen;

compare said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen; and

reject said received message in response to said nonce value falling outside said acceptance window.

11. The apparatus according to claim 10, wherein said controller is further configured to designate said nonce value as said largest nonce value yet seen in response to said nonce value exceeding said largest nonce value yet seen.

12. The apparatus according to claim 10, wherein said controller is further configured to adjust an acceptance window in response to said largest nonce value yet seen in response to said nonce value exceeding said largest nonce value yet seen.

13. The apparatus according to claim 10, wherein said controller is further configured to replace said largest nonce value yet seen with said nonce value in response to said nonce value exceeding said largest nonce value yet seen.

14. The apparatus according to claim 10, wherein said controller is further configured to designate said received message as part of a replay attack.

15. The apparatus according to claim 10, wherein said controller is further configured to:

compare said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

reject said received message in response to an outcome of said comparison of said nonce value to said window mask value being true.

16. The apparatus according to claim 15, wherein said controller is further configured to designate said received message as part of a replay attack

17. The apparatus according to claim 10, wherein said controller is configured to:

compare said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

accept said received message in response to an outcome of said comparing of said nonce value to said window mask value being false.

18. The apparatus according to claim 17, wherein said controller is further configured to mark said nonce value as a nonce value seen.

19. A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of processing messages, said one or more computer programs comprising a set of instructions for:

comparing a nonce value of a received message and a largest nonce value yet seen;

comparing said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen; and

rejecting said received message in response to said nonce value not falling within said acceptance window.

20. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating said nonce value as a nonce value seen in response to said nonce value exceeding said largest nonce value yet seen..

21. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

replacing said largest nonce value yet seen with said nonce value in response to said nonce value exceeding said largest nonce value yet seen.

22. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

adjusting an acceptance window based on said nonce value in response to said nonce value exceeding said largest nonce value yet seen.

23. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating said received message as a replay attack.

24. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

rejecting said received message in response to an outcome of said comparison of said nonce value to said window mask value being true.

25. The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

designating said received message as part of a replay attack.

26. The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window; and

accepting said received message in response to an outcome of said comparing of said nonce value to said window mask value being false.

27. The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

designating said nonce value as a nonce value seen.

28. A system for processing messages in a peer-to-peer configuration, comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a secure communication module configured to be executed by said first peer and second peer, wherein said secure communication module is configured to:

compare said nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen;

compare said nonce value to a replay mask; and

accept said received packet in response to said comparison of said nonce value and said replay mask being false.

29. The system according to claim 28, wherein said secure communication module is further configured to designate said nonce value as said largest nonce value yet seen in response to said nonce value exceeding said largest nonce value yet seen.

30. The system according to claim 28, wherein said secure communication module is further configured to adjust said filter based on said largest nonce value yet seen in response to said nonce value exceeding said largest nonce value yet seen.

31. The system according to claim 28, wherein said secure communication module is further configured to reject said received packet in response to said nonce value falling outside said filter.

32. The system according to claim 31, wherein said secure communication module is further configured to designate said received packet as part of a replay attack.

33. The system according to claim 32, wherein said secure communication module is further configured to reject said received packet in response to said comparison of said nonce value and said replay mask being true.

34. The system according to claim 33, wherein said secure communication module is further configured to designate said received packet as part of a replay attack.

35. The system according to claim 28, wherein said secure communication module is further configured to reject said received packet in response to said nonce value fails to fall within said filter and said secure communication module is further configured to designate said received packet as part of a replay attack.

36. An interceptor device for processing messages, said interceptor device comprising:

a network interface;

an expected sequence register configured to enumerate an expected sequence number of a packet received from a second network device;

a memory configured to store a replay mask; and

a controller, wherein said controller is configured to:

compare said nonce value to a filter in response to a sequence number of a received packet via said network interface does not exceed a largest sequence number yet seen retrieved from said expected sequence register;

compare said sequence number to said replay mask retrieved from said memory; and

accept said received packet in response to said comparison of said sequence number and said replay mask is false.

37. The interceptor device according to claim 36, wherein said controller is further configured to designate said sequence number as said largest sequence number yet seen in response to said sequence number exceeding said largest sequence number yet seen.

38. The interceptor device according to claim 36, wherein said controller is further configured to adjust said filter based on said largest sequence number yet seen in response to said sequence number exceeding said largest sequence number yet seen.

39. The interceptor device according to claim 36, wherein said controller is further configured to reject said received packet in response to said sequence number falling outside said filter.

40. The interceptor device according to claim 36, wherein said controller is further configured to designate said received packet as part of a replay attack.

41. The interceptor device according to claim 36, wherein said controller is further configured to reject said received packet in response to said comparison of said sequence number and said replay mask being true.

42. The interceptor device according to claim 41, wherein said controller is further configured to designate said received packet as part of a replay attack.

43. The interceptor device according to claim 36, wherein said controller is further configured to reject said received packet in response to said sequence number falling outside said filter and said controller is further configured to designate said received packet as part of a replay attack.